Application #09/646,640
Amendment dated August 18, 2005

Amendments to the claims:

1. (cancelled).

2. (cancelled)

3. (cancelled)

4. (cancelled)

5. (cancelled)

6. (cancelled)

7. (cancelled)

8. (cancelled)

9. (cancelled)

Page 2 of 12

M481-3 Amendment 1.0

1   10. (currently amended) Data protection method, ~~for protecting data~~
2   ~~elements processed by a microprocessor in a chip card from~~
3   ~~discovery by analysis of the microprocessor's electric power~~
4   ~~consumption~~ said method using a cryptographic algorithm for
5   executing operations for processing ~~said~~ data elements so as to
6   generate encrypted information, said method comprising:
7   randomly modifying the order of execution of operations from
8   one cycle to another, a cycle being a complete execution cycle of
9   the algorithm or an intermediate cycle of a group of operations,
10   said operations being operations whose order of execution relative
11   to the others does not affect the result, <u>thereby protecting said data</u>
12   <u>elements processed by a microprocessor in a chip card from</u>
13   <u>discovery by analysis of the microprocessor's electric power</u>
14   <u>consumption.</u>

1   11. (previously presented) The protection method according to claim
2   10, wherein the modified order of execution of operations include
3   permutation of bits of a message block before permutation of bits of
4   a key, and vice versa.

1   12. (previously presented) The protection method according to claim
2   10, wherein the modified order of execution of operations include
3   modifying the order of processing quartets making up a data
4   element.

1   13. (previously presented) The protection method according to claim
2   10, wherein the modification of the order of execution of operations
3   is random.

M481-3 Amendment 1.0

1   14. (new) Data protection method, said method using a cryptographic

2   algorithm for executing operations for processing data elements so

3   as to generate encrypted information, said method comprising:

4   using a symmetric cryptographic algorithm of the DES-type with a

5   permutation step, said permutation step including a random

6   determination of a processing order of the bits for the execution of

7   the permutation step, thereby protecting said data elements

8   processed by a microprocessor in a chip card from discovery by

9   analysis of the microprocessor's electric power consumption.

1   15. (new) The data protection method of Claim 14 wherein the

2   cryptographic algorithm for executing operations for processing

3   data elements includes a group of operations executed repeatedly.

Page 4 of 12

M481-3 Amendment 1.0